



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,726	01/14/2000	SHARON S. LIU	5437-106	8758

29989 7590 06/08/2004

HICKMAN PALERMO TRUONG & BECKER, LLP  
1600 WILLOW STREET  
SAN JOSE, CA 95125

EXAMINER

KLIMACH, PAULA W

ART UNIT PAPER NUMBER

2135

DATE MAILED: 06/08/2004

14

Please find below and/or attached an Office communication concerning this application or proceeding.

St

# Office Action Summary

Application No.

09/483,726

Applicant(s)

LIU ET AL.

Examiner

Paula W Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE \_\_\_\_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 22 March 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-33 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_.

## **DETAILED ACTION**

### ***Response to Amendment***

This office action is in response to the request for reconsideration filed on 3/22/04 (Paper No. 13). Original application contained Claims 1-33. The amendment filed on request for consideration have been entered and made of record. Therefore, presently pending claims are 1-33.

### ***Response to Arguments***

Applicant's arguments filed 3/22/04 have been fully considered but they are not persuasive because reasons given in the new grounds of rejection.

The examiner asserts that the prior art does teach or suggest the subject matter broadly recited in independent Claims 1, 7, 12, 18, 23, 29. Dependent Claims 2-6, 8-11, 13-17, 19-22, 24-28 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action (Paper No. 14). The examiner has considered all the applicants arguments filed on 3/22/04, however due to the new prior art discovered the examiner rejections for claims 1-33 are respectfully as shown in this office action (Paper No. 14).

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2135

1. Claims 1-6, 12-17, and 23-28 rejected under 35 U.S.C. 102(e) as being anticipated by Jalili (U.S Patent 6,209,104 B1).

In reference to claims 1, 12, and 23, Jalili discloses a method, apparatus, and computer readable medium for verifying the legitimacy of an untrusted mechanism, comprising: submitting a first set of information and a second set of information to an untrusted mechanism in a sequence that is unpredictable to the untrusted mechanism (column 6 lines 32-48). The sequence of icons or data positions that do not correspond to the users password are the second sequence and the once that correspond to the users password are the first set. Receiving a response from the untrusted mechanism for each submission of either said first set of information or said second set of information (column 8 lines 1-15). Determining whether each response received from the untrusted mechanism is a correct response (column 8 lines 5-14). In response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate (column 8 lines 14-15). The response must be correct to be allowed access therefore an incorrect response would not allow access therefore indicating an illegitimate, or untrusted mechanism.

2. Claims 2-6, 13-17, and 24-28 are rejected as the rejection in claims 1, 12 respectively above.

In reference to claims 2, 3, 13, 14, 24, and 25, wherein said sequence is generated randomly. The sequence is generated using a random number generator (column 8 lines 20-32).

In reference to claim 4, 15, and 26, wherein said sequence includes at least one submission of said first set of information and at least one submission of said second set of

Art Unit: 2135

information (column 6 lines 32-48). The sequence of icons or data positions that do not correspond to the users password are the first sequence and the once that correspond to the users password are the second set.

In reference to claims 5, 16, and 27, wherein said first set of information is designed to solicit a first proper response from the untrusted mechanism, and said second set of information is designed to solicit a second proper response from the untrusted mechanism, and wherein determining whether each response received from the untrusted mechanism is a correct response comprises: where the set of information submitted to the untrusted mechanism was said first set of information, determining whether the response from the untrusted mechanism is said first proper response (column 6 lines 31-49); and where the set of information submitted to the untrusted mechanism was said second set of information, determining whether the response from the untrusted mechanism is said second proper response (column 8 lines 14-15). The first set of information would be the information representing the user's password and the second set of information would be all the other information that does not represent the user's password.

In reference to claim 6, 17, and 28, wherein said first proper response is an affirmative response, and wherein said second proper response is a negative response (column 8 lines 14-15).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 7-11, 18-22, and 29-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jalili in view of Shostack et al (U.S Patent 6,298,445 B1).

In reference to claims 7, 10-11, 18, 21-22, 29, and 32-33, Jalili discloses a method, apparatus, and computer readable medium for verifying the legitimacy of an untrusted mechanism, comprising: submitting a first information and second information to an untrusted mechanism in a sequence that is unpredictable to the untrusted mechanism, said first information being known to be verifiable, and said information being known to be unverifiable (column 6 lines 32-48); receiving a response from the untrusted mechanism for each submission of either said first information or said second information (column 8 lines 1-15); determining whether each response received from the untrusted mechanism is a correct response (column 8 lines 14-15); and in response to a determination that any of the responses from the untrusted mechanism is an incorrect response, determining the untrusted mechanism to not be legitimate. The response must be correct to be allowed access therefore an incorrect response would not allow access therefore indicating an illegitimate, or untrusted mechanism.

Jalili does not expressly teach the information used for verification being a digital signature.

However, Shostack discloses the use of digital signatures to authenticate the integrity of the software enhancement (column 10 lines 21-24).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the digital signature for the information to identify the user as disclosed by Shostack in the system disclosed by Jalili. Therefore the correct digital signature would be represented by the first set of icons and the other icons would represent digital signatures that are unverifiable. One of ordinary skill in the art would have been motivated to do this because the digital signature facilitates the authentication of the software by using a cryptographic function computed as a message and a user's private key. The signature function produces a value unique to the private key and the finger print value being signed. The private key has a mathematically related public key that anyone may use to verify the signature created by the private key (Shostack column 11 lines 10-17).

*In reference to claims 10, 21, and 32, wherein said sequence includes at least one submission of said first signature and at least one submission of said second signature (Jalili column 6 lines 32-48):* The reference Jalili discloses the use of a plurality of icons, as a result the icons would fall into two groups; icons that represent the password and icons that do not represent the password. Jalili does not expressly disclose the information to include digital signatures. Shostack discloses the use of digital certificates for authentication.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the digital signature for the information to identify the user as disclosed by Shostack in the system disclosed by Jalili. Therefore the correct digital signature would be represented by the first set of icons and the other icons would represent digital signatures that are

Art Unit: 2135

unverifiable. One of ordinary skill in the art would have been motivated to do this because the digital signature facilitates the authentication of the software by using a cryptographic function computed as a message and a user's private key. The signature function produces a value unique to the private key and the finger print value being signed. The private key has a mathematically related public key that anyone may use to verify the signature created by the private key (Shostack column 11 lines 10-17).

*In reference to claims 11, 22, and 33*, wherein determining whether each response received from the untrusted mechanism is a correct response comprises: where the information submitted to the untrusted mechanism was said from the icons describing the user's password, determining whether the response from the untrusted mechanism matches the user's password (Jalili column 8 lines 5-14). Determining whether the information is taken from the matches the information that describes the user's password.

Jalili does not disclose the information sent to the user being digital signatures

Shostack discloses the use of digital signatures for authentication.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the digital signature as disclosed by Shostack in the system disclosed by Jalili so that the icons represent the digital signature instead of the password. One of ordinary skill in the art would have been motivated to do this because the digital signature facilitates the authentication of the software by using a cryptographic function computed as a message and a user's private key. The signature function produces a value unique to the private key and the finger print value being signed. The private key has a mathematically related public key that



Art Unit: 2135

anyone may use to verify the signature created by the private key (Shostack column 11 lines 10-17).

4. Claims 8-9, 19-20, and 30-31 are rejected as in the rejection for claims 7, 18, and 29 respectively above.

In reference to claims 8, 19, and 30, wherein said sequence is generated randomly (column 8 lines 20-32).

In reference to claims 9, 20, and 31, wherein said sequence is generated using a random number generator. The random sequence is generated using a random number generator or a pseudo random number generator.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (703) 305-8421.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK

June 1, 2004



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER